



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/933,995	08/21/2001	Saed G. Younis	010356	7655

23696 7590 02/22/2005

Qualcomm Incorporated  
Patents Department  
5775 Morehouse Drive  
San Diego, CA 92121-1714

EXAMINER
----------

SCHUBERT, KEVIN R

ART UNIT	PAPER NUMBER
----------	--------------

2137

DATE MAILED: 02/22/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

09/933,995

Applicant(s)

YOUNIS, SAED G.

Examiner

Kevin Schubert

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 21 August 2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-13 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-13 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 21 August 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)                        | 4) <input type="checkbox"/> Interview Summary (PTO-413)                     |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)               | Paper No(s)/Mail Date. _____  |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date <u>06092003</u> .  | 6) <input type="checkbox"/> Other: _____                                    |

Art Unit: 2137

### DETAILED ACTION

Claims 1-13 have been considered.

#### *Claim Objections*

5            Claims 3 and 4 are objected to because of the following informalities: "Tijndael" should be "Rijndael". Appropriate correction is required.

#### *Claim Rejections - 35 USC § 102*

10            (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or  
15            (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

             Claims 1 and 7-13 are rejected under 35 U.S.C. 102(e) as being anticipated by Hokkanen, PCT International Publication Number WO 99/53621.

20

             As per claims 1 and 9-13, the applicant describes a method for enabling a mobile apparatus for call processing comprising the following limitations:

             a) encrypting a random number at the mobile apparatus (Page 10, lines 23-27; Page 9, lines 18-23; Page 9, line 35 to Page 10, line 3);

25            b) sending the random number from the mobile apparatus to a charging apparatus (Page 10, lines 23-27);

             c) encrypting the random number at the charging apparatus (Page 10, lines 23-27; Page 8, lines 15-16);

30            d) receiving at the mobile apparatus the encrypted random number from the charging apparatus (Page 10, lines 23-27);

Art Unit: 2137

e) enabling the mobile apparatus based on a comparison of the encrypted random number at the mobile apparatus with the encrypted random number received from the charging apparatus (Page 10, lines 23-27);

Hokkanen describes a system for enabling a mobile phone for call processing. The system allows a mobile phone operating as a cell phone to operate as a cordless house phone when it is placed in a charging apparatus located in a home base station (Abstract).

Registration of the mobile apparatus begins when it is placed on the charging apparatus and the home base station feeds a random number RAND, an algorithm known as SRES which is an encryption of the random number with a subscriber specific key  $K_i$  (Page 8, lines 15-16), and a connection specific key  $K_c$  into the memory of the mobile device. The above registration process is described in Page 9, line 26 to Page 10, line 27. Enabling of the mobile apparatus is accomplished when the mobile apparatus calls in to the home base station or receives a call from the home base station and authentication is established between the mobile phone and the home base station charging unit. Authentication, or the enabling, can take place on either the home base station or the mobile phone. The examiner uses the authentication on the mobile phone because the claims read on authentication at the mobile phone.

Regarding parts a) and b), after registration has occurred, the mobile phone is taken away from the home base station charger. During authentication for making a call or receiving a call, the mobile phone sends the home base station charger a random number (Page 10, lines 23-27). As described throughout the patent (Page 9, lines 13 to line 23), the ciphering key ( $K_c$ ) which is registered with the mobile station in addition to the random number (RAND) and the encryption of the random number using  $K_i$  (SRES) (Page 9, lines 35-36), is a connection-specific ciphering key used to encrypt the RAND and the SRES for transmission between the mobile phone and the home base station. The RAND is encrypted with the ciphering key  $K_c$  when it is sent between the mobile phone and the home base station.

Regarding parts c) and d), the encryption of the random number at the charging apparatus is the SRES, which is the encryption of the random number with  $K_i$ , the subscriber specific key. The home base station charging apparatus sends the mobile phone the SRES.

Art Unit: 2137

Regarding part e), a comparison of the SRES received with the SRES stored in the memory of the mobile phone authenticates the home base station for enablement of operation.

Regarding claims 10 and 12, the use of a processor in the mobile apparatus and the charging apparatus is inherent. Without a processor the mobile phone and the charging unit  
5 would not be able to perform such functions as encryption and comparison.

As per claims 7 and 8, the applicant describes the method of claim 1, which is met by Hokkanen (see above), with the following limitation which is also met by Hokkanen:

Wherein the enabling further includes enabling the mobile apparatus while the mobile  
10 apparatus is located within a predetermined distance from the charging apparatus that is dedicated to the mobile apparatus (Page 6, lines 26-33);

The mobile phone is enabled to receive or place calls as a cordless phone after authentication has taken place through a random number exchange between the mobile phone and the home base station charging apparatus. However, the mobile phone also has information  
15 programmed into its memory which cancels the enablement with the home base station once the mobile phone moves outside the predetermined range of the home base station.

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness  
20 rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been  
25 obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 2 and 5 are rejected under 35 U.S.C. 103(a) as being unpatentable over  
30 Hokkanen in view of Menezes (Menezes, Oorschot, Vanstone: Handbook of Applied

Art Unit: 2137

Cryptography, CRC Press Series on Discrete Mathematics and its Applications, CRC Press, 1997, Pages 397-400).

As per claims 2 and 5, the applicant describes the method of claim 1, which is met by

5 Hokkanen (see above), with the following limitation which is met by Menezes:

Wherein the random number is an encrypted system time (Page 399-400);

Hokkanen describes all the limitations of claim 1, the independent claim. However,

Hokkanen does not describe a process for sending an encrypted system time. In paragraph [1028], the applicant describes that a system time may be sent as a time limitation for

10 enablement: "The register may be loaded with the system time whenever the mobile is successfully enabled for call processing. When a call-processing request is received, the mobile may compare the content of the register with the current system time. If the difference is less than a predetermined time period, the time has not expired and the call processing may be allowed. If the predetermined time period has expired, the mobile may be disabled to handle the requested call processing, and may return to idle state" (Applicant: [1028].

Menezes discloses that using an encrypted system time is an effective way to incorporate "time-limited access privileges" (Page 399). The timestamp, which may be cryptographically binded to a message (encrypted), allows for an acceptable window for a message to be received in.

20 It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Menezes with those of Hokkanen and incorporate the use of an encrypted system time to allow enablement only for a certain amount of time for security reasons.

Regarding claim 5, the enabling of the mobile apparatus for a predetermined period of time is the acceptable window as described above.

25

Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hokkanen in view of Menezes in further view of Moshopoulos, (Moshopoulos, Nikos; Chaniotakis, Eleftherios. A Survey

Art Unit: 2137

of Cryptography Algorithms- Trends and Products. National Technical University of Athens. 2000. Pages 1-28).

As per claim 3, the applicant describes the method of claim 2, which is met by Hokkanen  
5 in view of Menezes (see above), with the following additional limitation which is met by  
Moshopoulos:

Wherein the encrypted system time is based on Rijndael 128-bit key encryption  
technique (Page 15);

Hokkanen in view of Menezes meets all the limitations of claim 2. However, Hokkanen in  
10 view of Menezes fails to disclose the use of Rijndael 128-bit key encryption.

Moshopoulos's paper describes a survey of common cryptography algorithms.  
Moshopoulos also discloses that Rijndael 128-bit key encryption is one of the fastest encryption  
algorithms (Page 15).

It would have been obvious to one of ordinary skill in the art at the time the invention was  
15 filed to incorporate the ideas of Moshopoulos with those of Hokkanen in view of Menezes and use  
Rijndael 128-bit key encryption because it is a fast encryption algorithm.

Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hokkanen in view  
of Moshopoulos.

20

As per claim 4, the claim is rejected on the same grounds as claim 3 above except for the  
fact that claim 3 is rejected under Hokkanen in view of Menezes in further view of Moshopoulos  
and claim 4 is rejected under Hokkanen in view of Moshopoulos.

25

Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hokkanen in view  
of Blow, WO 99/53621.

Art Unit: 2137

As per claim 6, the applicant describes the method of claim 1, which is met by Hokkanen (see above), with the following limitation which is met by Blow:

Wherein the enabling further includes enabling the mobile apparatus while the mobile apparatus is positioned on the charging apparatus that is dedicated to the mobile apparatus

5 (Blow: Page 5, lines 27-36; Page 1, lines 15-23; Page 4, lines 3 to 11; Fig 1);

Hokkanen describes all the limitations of claim 1, the independent claim. However, in Hokkanen's system the enablement of the apparatus takes place through a wireless connection between the mobile apparatus and the home base station charging apparatus. Thus, Hokkanen lacks the limitation that the enablement takes place on the home base station charging

10 apparatus.

Blow describes a system similar to Hokkanen's system and the applicant's system in which a wireless communication device, such as a "portable telephone" (Page 1, line 16) authenticates an accessory, such as a "battery charger" (Page 1, line 17). In Figure 1, the wireless communication device, or mobile phone, is 100 and the accessory, or charger, is 102.

15 However, in Blow's system the interface 112 can be a wireless interface or a physical interface such as the mobile phone being physically connected to the accessory (Page 4, lines 3 to 11). The authentication which takes place between the mobile phone and the accessory charging unit is similar to that of Hokkanen's and the applicant's (Page 5, lines 27-36).

20 It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Blow with those of Hokkanen and authenticate the mobile phone on the home base station charging unit in the event that a person wants to make or receive a call while the phone is being charged in the home base station.

25 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kevin Schubert whose telephone number is (571) 272-4239. The examiner can normally be reached on M-F 8:00-5:00.



Art Unit: 2137

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent  
5 Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

10  
\*\*\*



**ANDREW CALDWELL**  
**SUPERVISORY PATENT EXAMINER**

15

20